



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/007,446

12/05/2001

Roy F. Brabson

RSW920010221US1

3354

25259

7590

10/25/2006

IBM CORPORATION

3039 CORNWALLIS RD.

DEPT. T81 / B503, PO BOX 12195.

REASEARCH TRIANGLE PARK, NC. 27709

EXAMINER

SANDOVAL, KRISTIN D

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 10/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

OCT 25 2006

Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/007,446
Filing Date: December 05, 2001
Appellant(s): BRABSON ET AL.

David C. Hall
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed August 9, 2006 appealing from the Office
action mailed March 23, 2006

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

NEW GROUND(S) OF REJECTION

The amendment after final included the limitation of dependent claim 3 incorporated into the limitations of independent claims 1, 17 and 18. Claim 3 had previously been rejected as a 35 USC 103 rejection. However, after further consideration, claims 1, 17 and 18 are rejected as a 35 USC 102(b) rejection.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Art Unit: 2132

5,029,206	MARINO, JR. ET AL.	7-1991
6,131,163	WIEGEL	10-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

NEW GROUND(S) OF REJECTION

The amendment after final included the limitation of dependent claim 3 incorporated into the limitations of independent claims 1, 17 and 18. Claim 3 had previously been rejected as a 35 USC 103 rejection. However, after further consideration, claims 1, 17 and 18 are rejected as a 35 USC 102(b) rejection.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

1. Claims 1, 17 and 18 rejected under 35 U.S.C. 102(b) as being anticipated by Marino, Jr. et al. (Marino), U.S. Patent No. 5,029,206.

As per claims 1, 17 and 18:

Marino discloses a method of improving security processing in a computer network comprising the steps of:

providing security processing in an operating system kernel (3:12-25, wherein encryption is the security processing at the kernel);

Art Unit: 2132

providing an application program which makes use of the operating system kernel during execution (4:1-9);

providing security policy information that is usable for more than one executing application program specifying at least one condition under which the means for performing security processing is to be activated (7:36-66 wherein the provided parameters are the security policy information and the information the parameters provide is the at least one condition under which the means for performing security processing is to be activated. 8:58-9:38, wherein, since the black application software and the receiving application must receive the cryptographic association which contains the security policy information in the form of parameters and uses the cryptographic association to execute their applications in order to decrypt the data, the security policy information in the form of parameters are usable for more than one executable application program);

executing the application program (5:41-51 wherein the applications are executed when requests are made); and

selectably encrypting at least one communication of the executing application program using the provided security processing in the operating system kernel, under conditions specified by the security policy information (7:36-66).

As per claims 17 and 18, these are system and computer program versions respectively of the claimed apparatus discussed above in claim 1 wherein all claimed limitations have also been addressed and/or cited as set forth above.

Art Unit: 2132

2. Claims 2-8, 10, 11 and 14 rejected under 35 U.S.C. 103(a) as being unpatentable over Marino as applied to claims 1 above, and further in view of Wiegel, (U.S 6,131,163).

As per claim 2:

Wiegel substantially teaches a method wherein the security policy information is stored in a security repository (9:23-27).

As per claim 4:

Wiegel substantially teaches a method wherein the conditions include network addresses (9:41-55).

As per claim 5:

Wiegel substantially teaches a method wherein the network addresses specify one or more of server addresses and destination addresses (9:41-55).

As per claim 6:

Wiegel substantially teaches a security policy tree that includes the condition of a source or destination address. It would have been an obvious modification to include a range of destination addresses (9:41-55).

As per claim 7:

Wiegel substantially teaches a method wherein the conditions include one or more port numbers and/or one or more port number ranges (9:26-30).

As per claim 8:

Wiegel substantially teaches a method wherein the conditions include one or more job names (9:41-55, wherein network service acts as job names).

As per claim 10:

Wiegel substantially teaches a method further comprising the step of checking the security policy information when the executing application program establishes a connection, and wherein the selectably securing step communicates on that connection according to a result of the checking step (10:15-49).

As per claim 11:

Wiegel substantially teaches a method whereby communications from the executing application program may be secured even though the provided application program has no code for security processing (10:15-49).

As per claim 14:

Wiegel substantially teaches a method wherein the provided security processing operates in a Transmission Control Protocol layer of the operating system kernel (3:38-46).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the invention of Marino to utilize the invention of Wiegel because Wiegel offers increased assurance that communications coming into and out of individual computers over a network are authentic (1:47-67) which would improve upon Marino's invention of increasing the security of communications amongst computers at the kernel level within a network (1:6-39).

3. Claims 9 and 13 rejected under 35 U.S.C. 103(a) as being unpatentable over Marino as applied to claim 1 above and further in view of Winiger, U.S. Patent No. 5,845,068.

As per claim 9:

Art Unit: 2132

Marino fails to teach identifiers used as conditions for the security policy. However, Winiger discloses utilizing source and destination machine identification numbers which would correspond to client identifiers since a destination or source machine would be a client (8:6-39).

As per claim 13:

Marino fails to teach a security policy governing communications on sockets of a port. However, the use of communications over sockets and ports was well known in the art at the time of applicant's invention as illustrated by Winiger. Winiger discloses the use of multiple sockets having the same port number (9:66-10:2) and utilizing the security level of the user to determine whether communication can occur on that socket having that port number which is similar to the security level negotiations taught by Marino (7:67-8:12).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to improve upon the invention of Marino with the use of sockets and ports between network devices as shown in Winiger because Marino was already using network and transport layer security and it would have been obvious to use the improvements such as Winigers in order to continue to make the invention of Marino more secure (7:51-54).

4. Claim 12 rejected under 35 U.S.C. 103(a) as being unpatentable over Marino as applied to claim 1 above further in view of Mod_SSL.

As per claim 12:

Wiegel fails to disclose a method wherein the provided application program includes invocation of one or more security directives, and further comprising the step of executing, during execution of the provided application program, one or more of the invoked security

Art Unit: 2132

directives. However, the Mod_SSL manual discloses a variety of security directives (lines 8-16, pg. 1 of chap. 3).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize security directives in order to have a better understanding of how a mod_ssl functionality is activated (lines 3-4, pg. 1 of chap. 3).

5. Claim 15 rejected under 35 U.S.C. 103(a) as being unpatentable over Marino as applied to claim 1 above further in view of Berg, PG Pub 2002/0116605.

As per claim 15:

Marino fails to teach a method wherein the provided security processing implements Secure Sockets Layer. However, SSL was well known in the art at the time of applicant's invention as exemplified by Berg.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize SSL because this is an obvious improvement to secure network communications that were utilized in Marino (7:51-57).

6. Claim 16 rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegel as applied to claim 1 above further in view of Dierk et al. (Dierk), RFC 2246.

As per claim 16:

TLS was well known in the art at the time the invention was made as exemplified by Dierks. It would have been an obvious modification, if using the invention for SSL, to upgrade and utilize TLS (pg. 5, item 3: Goals of this document).

(10) Response to Argument

Applicant's arguments with respect to claims 1, 17 and 18 have been considered but are moot in view of the new ground(s) of rejection as stated above. Since the rejection has been changed to a 35 USC 102(b) rejection as opposed to a 35 USC 103 rejection, the arguments with respect to the secondary reference (Wiegel, U.S. 6,131,163) are moot. However, the rebuttal pertaining to the combination of the references is still relevant to the dependent claims.

The Applicant has argued:

Accordingly, in the system of Marino, when a secure communication session is to be established, security information is passed from the application program to the security kernel. This is in direct contrast to Claim 1, which recites selectively encrypting a communication of an executing application program using security processing in the operating system kernel, under conditions specified by security policy information that is usable for more than one executing application program. Since the security processing of Marino is performed in response to security parameters passed by individual programs, the security processing of Marino is not performed under conditions specified by security policy information that is usable for more than one executing application program. Moreover, there is no indication in Marino that the parameters passed by an application to the security modules described therein are usable for more than one application program.

In response to applicant's argument, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in

Art Unit: 2132

order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. Claims 1, 17 and 18 state the limitation of, "providing security policy information that is usable for more than one executing program (emphasis added)". This is an intended use of the security policy information and the prior art structure disclosed by Marino consists of security parameters and they are capable of performing the intended use of being used for more than one executing application program as stated in the claims. Applicant insists that because the security parameters are passed by the application itself they cannot be used for another application besides the one passing the security parameters, however, the security parameters that are passed include cryptographic algorithms used, type of network security and one-way or two-way traffic encryption keys just to name a few. More than one application program could use the same cryptographic algorithm, network security and one-way or two-way traffic encryption keys.

In addition, Marino does indicate that the parameters are used for more than one application program. The security parameters are passed by a requesting application program in order to set up a cryptographic association and one of those parameters is the cryptographic algorithm to be used for both encryption and decryption (7:36-46). Therefore, the cryptographic algorithm used to encrypt the data coming from the requesting application must be passed to the *receiving* application, the application receiving the communications from the requesting application in order to decrypt the data coming from the requesting application, therefore, since the same security policy information is used with both the initial requesting application and the responding application and the black system software applications the security policy

Art Unit: 2132

information in the form of the security parameters is used for more than one application program (8:40-9:48).

Applicant further argues:

However, the combined system hypothesized in the Advisory Action is not the subject matter to which Claim 1 is directed. That is, Claim 1 is directed to securing communications of an application program, not securing a system against attacks outside a network. Thus, even if Marino and Wiegel were combined, it would simply provide the system of Marino with port-level security processing as described in Wiegel, and would not suggest a system that selectably encrypts a communication of an executing application program using provided security processing in the operating system kernel, under conditions specified by security policy information that is usable by more than one application program, as recited in Claim 1.

The specific references to Claim 1 are moot based on the new grounds of rejection disclosed above, therefore, this rebuttal is in reference to the combination of Marino and Wiegel as it would apply to the remaining dependent claims.

In response to applicant's argument, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

If the system as a whole is protected from attacks from outside the network then the communications of an application that makes up that system will be more secure. It would have been obvious to one of ordinary skill in the art that combining Marino and Wiegel would suggest more secure communications of a system's application programs if it is protected from unauthorized attacks and malicious code (1:51-55), which is what Wiegel would provide at the kernel level doing data security checks at the operating system level on data coming from the computer hardware that interfaces with the system to the network (1:64-67). If the system as a whole is not protected from an attack from outside the network such as malicious code or an attack, then the entire system is compromised, including the communications of an application program.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

(12) Conclusion

For the above reasons, it is believed that the rejections should be sustained.

This examiner's answer contains a new ground of rejection set forth in section (9) above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject to the new ground of rejection:

(1) Reopen prosecution. Request that prosecution be reopened before the primary examiner by filing a reply under 37 CFR 1.111 with or without amendment, affidavit or other evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of

Art Unit: 2132

rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR 41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be treated as a request that prosecution be reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 CFR 1.136(b) for extensions of time to reply for patent applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination proceedings.

Respectfully submitted,

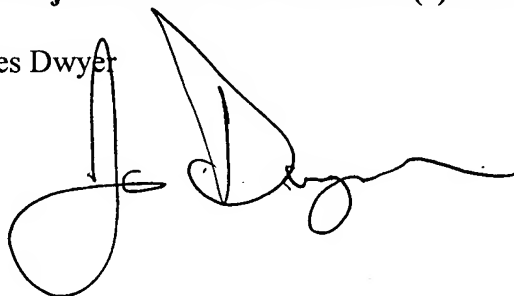
KDS 10/18/2006

KDS


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:

James Dwyer



Art Unit: 2132

Conferees:

Gilberto Barron 

Benjamin Lanier 